SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #17

Security Skills Assessment and Appropriate Training

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # # 17

"For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs."

CIS Top 20 Critical Security Controls

- Is your team well trained or does it lack fundamentals and often the advanced skills needed to perform their jobs?

CIS Controls™

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

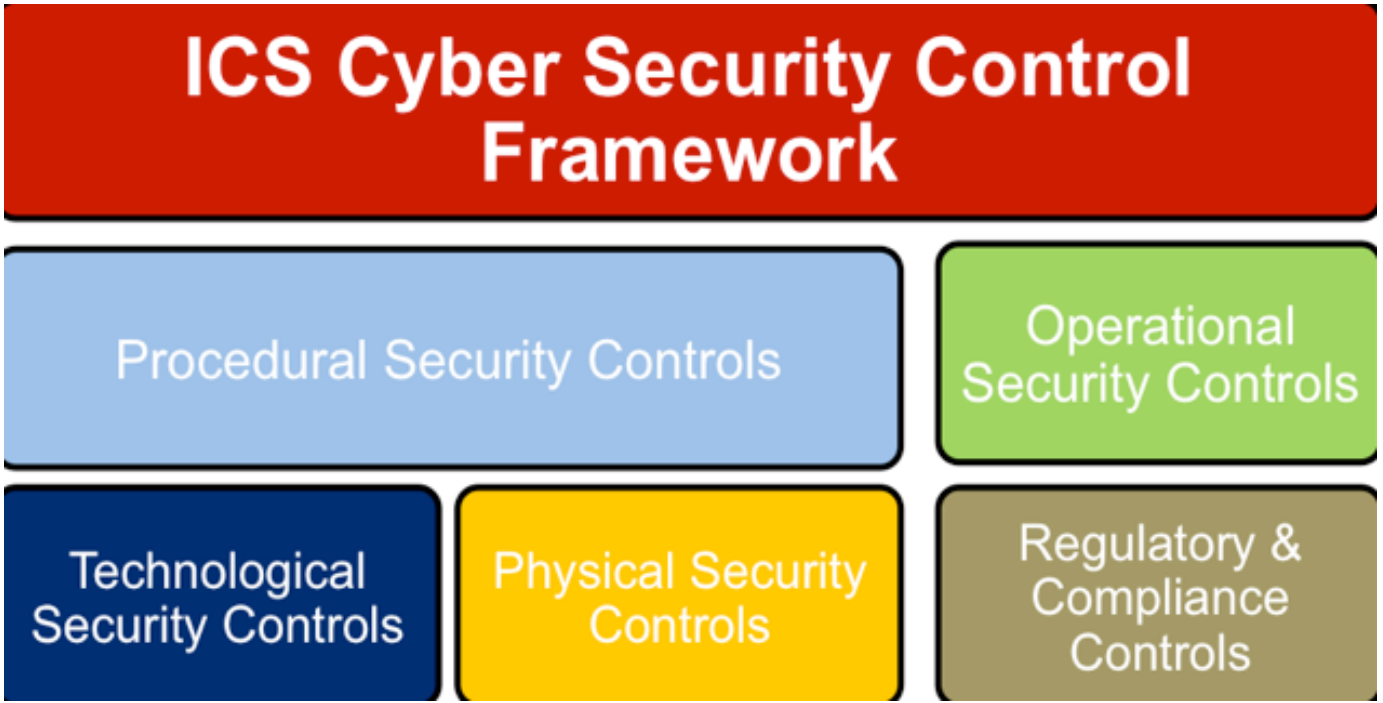
Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Top 20 Critical Security Controls



CIS Top 20 Critical Security Controls

- It is tempting to think of cyber defense primarily as a technical challenge but…..

CIS Top 20 Critical Security Controls

- **The Solution**
  - Continual security awareness training for all employees
  - Companies should develop and deliver enterprise-wide training for all employees

CIS Top 20 Critical Security Controls

- An effective enterprise-wide training program should take a holistic approach and consider policy and technology at the same time as the training of people

CIS Top 20 Critical Security Controls

- With technical controls in place, training can be focused concepts and skills that cannot be managed technically

CIS Top 20 Critical Security Controls

- NIST SP 800-50 Infosec Awareness Training https://csrc.nist.gov/publications/detail/sp/800-50/final
- EDUCAUSE https://library.educause.edu/search#?q=security%20awareness%20and%20training
- NCSA https://staysafeonline.org/
- SANS https://www.sans.org/security-awareness-training/resources

CIS Top 20 Critical Security Controls

- Such security awareness training should:
  - Focus on common methods of intrusion;
  - Be updated frequently to include new trends;
  - Be mandatory for all employees including senior leadership; and
  - Include metrics to track improvement.

CIS Top 20 Critical Security Controls

How can this control be implemented and its effectiveness measured?

- Organizations should develop security awareness training for various personnel job descriptions.
- The training should include specific, incident-based scenarios showing the threats an organization faces.
- The training should reflect proven defenses for the latest attack techniques.
- Organizations should devise periodic security awareness assessment quizzes, to be given to employees and contractors on at least an annual basis, determining whether they understand the information security policies and procedures for the organization, as well as their role in those procedures.
- Organizations should conduct periodic exercises to verify that employees and contractors are fulfilling their information security duties, by conducting tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller.

CIS Top 20 Critical Security Controls

- Great Groups to Join:
  - PaloAlto Fuel User Group
  - OWASP Chapters
  - Defcon
  - Sans

CIS Top 20 Critical Security Controls

- Do not dismiss the value of setting up a home lab of equipment or virtualized and ISO distributions to practice hacking and defending your home network.
  - The skills acquired away from work are often the skills that make the biggest difference.

CIS Top 20 Critical Security Controls

- The key to upgrading skills is measurement – not just with certification examinations

- Once the gaps have been identified, those employees who have the knowledge can be called upon to mentor the employees

CIS Top 20 Critical Security Controls

- Key Takeaways in Control 17
- **Less focus on metrics**.
  - This round of controls is focused more on just establishing a method to deliver continuous training while only highlighting a handful of the most common attack vectors.
- **Outsourcing continues to be ideal**.
  - Establishing an awareness training program from scratch will be a time-consuming process that may be better suited for a third-party to develop and deliver.

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress

CIS Top 20 Critical Security Controls

- Sample Gap questions

1. Are only authorized personnel documented and granted access to the organization's data assets?
2. Are background checks performed against all of the organization's personnel prior to granting access?
3. Are personnel properly trained in their responsibilities and in protecting the organization's data prior to being granted access to the organization's data?

CIS Top 20 Critical Security Controls

17.1	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
17.2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.
17.3	Implement an security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion.
17.4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.
17.5	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.

CIS Top 20 Critical Security Controls

17-1 PERFORM A SKILLS GAP ANALYSIS

- **Description**: Perform a skills gap analysis to understand the skills and behaviors to which workforce members are not adhering, using this information to build a baseline education roadmap.
  - **Notes**: Performing a true skills gap analysis across the organization is going to be a time-consuming process. If you are just starting out on your journey of security awareness training for the organization, it may be best to look for a third party for help.

CIS Top 20 Critical Security Controls

17-2 DELIVER TRAINING TO FILL THE SKILLS GAP

- **Description**: Deliver training to address the skills gap identified to positively impact workforce members' security behavior.
  - **Notes**: Delivering the training is just closing the loop from the first section. Delivering the training can be either in-person presentations or automated videos delivered through the web. The size and complexity of your organization will most likely determine which route you will want to go.

CIS Top 20 Critical Security Controls

17-3 IMPLEMENT A SECURITY AWARENESS PROGRAM

- **Description**: Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

  - **Notes**: There are a couple of bullet points to break down with this section. The first is that the training should be delivered on a regular basis. Security awareness, as well as information security as a whole, is not a one-time solution. Second is that employees need to exhibit the behavior and skills based on the training they receive. Showing employees 20 bullet pointed slides on the definitions of phishing isn't going to cut it. You need to make it fun and engaging then test them on what they learned after they have consumed the information.

CIS Top 20 Critical Security Controls

17-4 Validate and improve

- UPDATE AWARENESS CONTENT FREQUENTLY
- Description: Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.

  - Notes: The tactics, techniques, and procedures attackers use are changing constantly. The training should reflect new attacks which are gaining popularity. Circling back to the previous section, employees are going to tune out if they are receiving the same training every quarter. Providing new information will help make concepts stick.

CIS Top 20 Critical Security Controls

- 17-5 Use security skills assessments for each of the mission-critical roles to identify skills gaps.
  - Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday September 18th

CIC CSC # 18

Application Security